



Text Part Number: 78-5112-12

Release Notes for Cisco uBR7246 Universal Broadband Router for Cisco IOS Release 11.3 T

August 2, 1999

These release notes for the Cisco uBR7246 universal broadband router support Cisco IOS Release 11.3 T, up to and including Release 11.3(11)T. Cisco IOS Release 11.3(11)T is based on Cisco IOS Release 11.3. These release notes are updated as needed to describe new features, new memory requirements, new hardware support, and other important information regarding the operation of the Cisco uBR7246.

For a list of software caveats that apply to Release 11.3(11)T, refer to the *Caveats for Cisco IOS Release 11.3 T* document that accompanies these release notes. This caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM. For more information, refer to the “Caveats” section on page 20 of this document.

Use these release notes with the cross platform *Release Notes for Cisco IOS Release 11.3* located on CCO and the Documentation CD-ROM.

Contents

These release notes discuss the following topics:

- Introduction, page 2
- System Requirements, page 3
- New and Changed Information, page 8
- Important Notes, page 12
- Caveats, page 20
- Related Documentation, page 21
- Service and Support, page 26
- Cisco Connection Online, page 27
- Documentation CD-ROM, page 27

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Copyright © 1998-1999
Cisco Systems, Inc.
All rights reserved.

Introduction

This section contains information about the Cisco uBR7246 universal broadband router and Early Deployment Releases (ED) for the Cisco uBR7246.

Cisco Data-over-Cable Products

The Cisco uBR7246 universal broadband router and the Cisco uBR904 cable access router are based on the Data Over Cable Service Interface Specification (DOCSIS) standards. These standards are being developed by a consortium of cable television companies whose goal is to encourage vendors to develop interoperable data-over-cable products.

Cisco uBR7246 Universal Broadband Router

The Cisco uBR7246 universal broadband router is designed to allow two-way transmission of digital data over a hybrid fiber coaxial cable (HFC) network. The Cisco uBR7246 supports Internet Protocol (IP) routing with a wide variety of protocols and any combination of Ethernet, Fast Ethernet, High-Speed Serial Interface (HSSI), and Asynchronous Transfer Mode (ATM) media. The Cisco uBR7246 gives cable operators a cost-effective, scalable, and feature-rich interface between subscriber cable modems and the backbone data network.

Note The Cisco uBR7246 recently earned DOCSIS certification from CableLabs.

Cisco uBR904 Cable Modem

The Cisco uBR904 cable modem is the subscriber unit, a key component within a cable data system. The subscriber unit functions as the interface between the subscriber's personal computer and the cable operator's network within the subscriber's small office or home office.

For more information on Cisco uBR904, refer to the "Related Documentation" section on page 21.

Early Deployment Releases

These release notes describe the Cisco uBR7246 for Cisco IOS Release 11.3(11)T. Release 11.3 T is an Early Deployment (ED) release based on Release 11.3, and delivers fixes to software caveats and support for new hardware.

Table 1 briefly describes the features and availability of ED releases for the Cisco uBR7246.

Table 1 Early Deployment Releases for the Cisco uBR7246

ED Release	Maintenance Release	Availability	Additional Software Features	Additional Hardware Features
Release 11.3 NA	10	Now	—	• MC16C Modem Card
Release 11.3 T	11	Now	—	—
Release 12.0 XI	4	Now	Features from Release 11.3 NA	• MC16C Modem Card
Release 12.0 T	5	Now	Features from Release 12.0(4)XI	• MC16C Modem Card • MC14C Modem Card

System Requirements

This section describes the system requirements for Release 11.3 T and includes the following sections:

- Memory Requirements, page 3
- Hardware Supported, page 3
- Determining the Version of Your Software Release, page 4
- Upgrading to a New Software Release, page 4
- Feature Set Tables, page 5

Memory Requirements

Table 2 describes the memory requirements of the Cisco IOS feature sets for the Cisco uBR7246 universal broadband router for Release 11.3(11)T. Cisco uBR7246 universal broadband routers are shipped with a 16- or 20-MB Flash memory card.

Table 2 Memory Requirements for the Cisco uBR7246 Universal Broadband Router

Feature Set	Image Name	Required Flash Memory	Required DRAM Memory	Runs From	Feature Status
MCNS Two-Way	ubr7200-p-mz	16 MB Flash	32 MB DRAM	RAM	Added in 11.3(1)T

Hardware Supported

Cisco IOS Release 11.3 T supports the Cisco uBR7246 universal broadband router.

Cisco IOS Release 11.3 T also supports the MC11 cable modem cards installed in the Cisco uBR7246 universal broadband router. The MC11 cable modem cards provide connection to the HFC network, offering one upstream port and one downstream port. The cable modem card slots are numbered from top to bottom: cable modem card slot 3, slot 4, slot 5, and slot 6.

Table 3 lists the interfaces supported by the Cisco uBR7246 universal broadband router.

Table 3 Supported Interfaces on the Cisco uBR7246

Interface, Network Module, or Data Rate	Product Number ¹	Description	Platforms Supported
Ethernet	PA-4E	4-port Ethernet 10BaseT port adapter	Cisco uBR7246
	PA-8E	8-port Ethernet 10BaseT port adapter	Cisco uBR7246
	PA-FE-TX	1-port 100BaseTX Fast Ethernet port adapter	Cisco uBR7246
	PA-FE-FX	1-port 100BaseFX Fast Ethernet port adapter	Cisco uBR7246
Serial (continued)	PA-4T+	4-port synchronous serial port adapter	Cisco uBR7246
	PA-8T-232	8-port EIA/TIA-232 synchronous serial port adapter	Cisco uBR7246
	PA-8T-V35	8-port V.35 synchronous serial port adapter	Cisco uBR7246
	PA-8T-X21	8-port X.21 synchronous serial port adapter	Cisco uBR7246

Table 3 Supported Interfaces on the Cisco uBR7246 (continued)

Interface, Network Module, or Data Rate	Product Number ¹	Description	Platforms Supported
Serial (continued)	PA-4E1G-75	4-port unbalanced (75-ohm) E1-G.703/G.704 synchronous serial port adapter	Cisco uBR7246
	PA-4E1G-120	4-port balanced (120-ohm) E1-G.703/G.704 synchronous serial port adapter	Cisco uBR7246
High Speed Serial Interfaces (HSSI)	PA-H	1-port HSSI port adapter	Cisco uBR7246
ATM	PA-A1-OC3SMI	1-port ATM OC-3c/STM-1 single-mode intermediate reach port adapter	Cisco uBR7246
	PA-A1-OC3MM	1-port ATM OC-3c/STM-1 multimode port adapter	Cisco uBR7246
	PA-A2-4E1XC-OC3SM	5-port ATM CES ² (4 E1 120-ohm CBR ³ ports and 1 OC-3 ATM single-mode port) port adapter	Cisco uBR7246
	PA-A2-4E1XC-E3ATM	5-port ATM CES ² (4 E1 120-ohm CBR ³ ports and 1 E3 ATM port) port adapter	Cisco uBR7246
	PA-A2-4T1C-OC3SM	5-port ATM CES ² (4 T1 CBR ³ ports and 1 OC-3 ATM single-mode port) port adapter	Cisco uBR7246
	PA-A2-4T1C-T3ATM	5-port ATM CES ² (4 T1 CBR ³ ports and 1 T3 ATM port) port adapter	Cisco uBR7246
Packet-Over-SONET (POS)	PA-POS-OC3SML	1-port POS OC-3 single-mode, long reach port adapter	Cisco uBR7246
	PA-POS-OC3SMI	1-port OC3 single-mode, intermediate reach port adapter	Cisco uBR7246
	PA-POS-OC3MM	1-port POS OC3 multimode port adapter	Cisco uBR7246

1 Refer to the Documentation CD-ROM or <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com> for the most current list of supported port adapters.

2 CES = circuit emulation services.

3 CBR = constant bit rate.

Determining the Version of Your Software Release

To determine the version of Cisco IOS software currently running on the Cisco uBR7246, log in to the router and enter the **show version EXEC** command. The IOS version number is displayed on the second line as indicated in the sample output shown below:

```
router>show version
Cisco Internetwork Operating System Software
IOS (tm) 7246 Software (C7246-JS-L), Version 11.3(11)T, RELEASE SOFTWARE
```

The output includes additional information such as processor revision numbers, memory amounts, hardware IDs, and partition information.

Upgrading to a New Software Release

For generic information on upgrading to a new software release, refer to the *Cisco IOS Software Release Upgrade Paths and Packaging Simplification* product bulletin located on CCO.

From the CCO home page, click on this path:

Service & Support: Product Bulletins: Software

Under **Cisco IOS 11.3**, click on **Cisco IOS Software Release 11.3 Upgrade Paths (#703: 12/97)**.

4 Release Notes for Cisco uBR7246 Universal Broadband Router for Cisco IOS Release 11.3 T

The *Cisco IOS Software Release Upgrade Paths and Packaging Simplification* product bulletin does not contain information specific to Cisco IOS Release 11.3 T, but provides generic upgrade information that may apply to Cisco IOS Release 11.3 T.

Feature Set Tables

Cisco IOS software is packaged in software images consisting of feature sets—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Table 4 lists the Cisco IOS software feature sets available for the Cisco uBR7246 in Cisco IOS Release 11.3 T, up to and including Release 11.3(11)T.

Table 4 Feature Sets Supported by the Cisco uBR7246

Feature Set	Feature Set Matrix Term	Software Image	Platforms
IP Standard Feature Sets			
MCNS Two-Way	Basic ¹	ubr7200-p-mz	Cisco uBR7246

¹ This feature is offered in the basic feature set.

Table 5 lists the features and feature sets available for the Cisco uBR7246 in Cisco IOS Release 11.3(11)T. Table 5 uses the following conventions:

- Yes—The feature is supported in the feature set.
- No—The feature is not supported in the feature set.
- In—Lists the Cisco IOS release that first introduced the feature. For example, (5) means a feature is introduced in 11.3(5)T. If a cell in this column is empty, the feature was included in the initial base release.

Table 5 Feature List by Feature Set for the Cisco uBR7246 for Cisco IOS Release 11.3(11)T

Feature	In	Feature Set
		MCNS Two-Way
Internet		
DRP Server Agent	(3)	Yes
IP Routing		
Easy IP (Phase 1)	(3)	Yes
Hot Standby Router Protocol (HSRP) over ISL in Virtual LAN Configurations	(3)	Yes
IP Type of Service and Precedence for GRE Tunnels	(4)	Yes
IP Enhanced IGRP Route Authentication	(3)	Yes
TCP Enhancements include: <ul style="list-style-type: none"> • TCP Selective Acknowledgment • TCP Timestamp 	(3)	No
LAN Support		
AppleTalk Access List Enhancements		No

Table 5 Feature List by Feature Set for the Cisco uBR7246 for Cisco IOS Release 11.3(11)T (continued)

Feature	In	Feature Set
		MCNS Two-Way
DECnet Accounting		No
IPX Named Access Lists		No
IPX SAP-after-RIP		No
NLSP Enhancements		No
NLSP Multicast Support		No
Management		
Cisco Call History MIB Command Line Interface	(3)	Yes
Cisco IOS Internationalization	(3)	Yes
Entity MIB, Phase 1	(3)	Yes
SNMPv2C	(3)	Yes
Virtual Profiles	(3)	Yes
Multimedia		
IP Multicast Load Splitting across Equal-Cost Paths	(3)	Yes
IP Multicast over ATM Point-to-Multipoint Virtual Circuits	(3)	Yes
IP Multicast over Token Ring LANs	(3)	Yes
Stub IP Multicast Routing	(3)	Yes
Quality of Service		
RTP Header Compression	(3)	Yes
Security		
Automated Double Authentication	(3)	Yes
Encrypted Kerberized Telnet		No
HTTP Security	(3)	Yes
Named Method Lists for AAA Authorization & Accounting	(3)	Yes
Per-User Configuration	(3)	Yes
Reflexive Access Lists	(3)	Yes
TCP Intercept		No
Vendor-Proprietary RADIUS Attributes	(3)	Yes
Switching		
AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs		No
CLNS and DECnet Fast Switching over PPP		No
DECnet/Vines/XNS over ISL include: <ul style="list-style-type: none"> • Banyan VINES Routing over ISL Virtual LANs • DECnet Routing over ISL Virtual LANs • XNS Routing over ISL Virtual LANs 		No
Fast-Switched Policy Routing	(3)	Yes
IPX Routing over ISL Virtual LANs		No

Table 5 Feature List by Feature Set for the Cisco uBR7246 for Cisco IOS Release 11.3(11)T (continued)

Feature	In	Feature Set
		MCNS Two-Way
VIP Distributed Switching Support for IP Encapsulated in ISL		No
Terminal Services		
Virtual Interface Template Service		No
Virtual Templates for Protocol Translation		No
WAN Optimization		
ATM MIB Enhancements		No
PAD Enhancements		No
PAD Subaddressing	(3)	Yes
WAN Services		
Bandwidth Allocation Control Protocol (BACP)	(3)	Yes
Enhanced Local Management Interface (ELMI)	(3)	Yes
Frame Relay Enhancements	(3)	Yes
Frame Relay MIB Extensions	(3)	Yes
Frame Relay Router ForeSight	(3)	Yes
ISDN Advice of Charge		Yes
ISDN Caller ID Callback		Yes
ISDN Multiple Switch Type		Yes
ISDN NFAS		Yes
LANE Per-subinterface Debug Messages		No
Layer 2 Forwarding—Fast Switching		No
Leased-Line ISDN at 128 kbps		No
MPPC		Yes
Multilink PPP Interleaving and Fair-Queuing Support		No
National ISDN Switch Types for BRI and PRI	(3)	Yes
PPP over ATM		No
Telnet Extensions for Dialout		No
VPDN MIB and Syslog facility	(3)	Yes
VPDN Tunnel Lookup Based on Dialed Number Information		No
X.25 Enhancements		Yes
X.25 on ISDN		No
X.25 Switching between PVCs and SVCs	(3)	Yes
X.28 Emulation		No

Optional feature set licenses for the Cisco uBR7246 universal broadband router are as follows:

- WAN Packet Protocols
 - ATM DXI
 - Frame Relay switching
 - Frame Relay SVC support (DTE)
 - Frame Relay traffic shaping
 - SMDS over ATM
 - X.25
 - X.25 switching
- Interdomain Routing
 - BGP
 - BGP4—Includes soft configuration, multipath support, and prefix filtering with inbound route maps
 - EGP for Internet scale routing

New and Changed Information

The following sections list the new features supported by the Cisco uBR7246 universal broadband router in Cisco IOS Release 11.3 T.

No New Features in Cisco IOS Release 11.3(11)T

No new features were introduced for the Cisco uBR7246 universal broadband router in Cisco IOS Release 11.3(11)T.

No New Features in Cisco IOS Release 11.3(10)T

No new features were introduced for the Cisco uBR7246 universal broadband router in Cisco IOS Release 11.3(10)T.

No New Features in Cisco IOS Release 11.3(9)T

No new features were introduced for the Cisco uBR7246 universal broadband router in Cisco IOS Release 11.3(9)T.

No New Features in Cisco IOS Release 11.3(8)T

No new features were introduced for the Cisco uBR7246 universal broadband router in Cisco IOS Release 11.3(8)T.

No New Features in Cisco IOS Release 11.3(7)T

No new features were introduced for the Cisco uBR7246 universal broadband router in Cisco IOS Release 11.3(7)T.

No New Features in Cisco IOS Release 11.3(6)T

No new features were introduced for the Cisco uBR7246 universal broadband router in Cisco IOS Release 11.3(6)T.

No New Features in Cisco IOS Release 11.3(5)T

No new features were introduced for the Cisco uBR7246 universal broadband router in Cisco IOS Release 11.3(5)T.

New Features in Cisco IOS Release 11.3(4)T

The following software enhancement was introduced in Cisco IOS Release 11.3(4)T and is available for the Cisco uBR7246.

IP Type of Service and Precedence for GRE Tunnels

Prior to the IP Type of Service and Precedence for GRE Tunnels feature, at generic route encapsulation-based tunnel endpoints, the Type of Service (TOS) bits (including precedence bits) were not copied to the tunnel or GRE IP header that encapsulates the inner packet. Instead, those bits were set to zero. This was not a problem unless the intermediate routers between two tunnel endpoints honored TOS or precedence bits, in which case those settings were ignored.

With the advent of virtual private network (VPN) and QoS applications, it is desirable to copy the TOS bits when the router encapsulates the packets using GRE. Thus, intermediate routers between tunnel endpoints can take advantage of the QoS features such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

New Features in Cisco IOS Release 11.3(3)T

The following hardware and software enhancements were introduced in Cisco IOS Release 11.3(3)T and are available for the Cisco uBR7246.

Named Method Lists for AAA Authorization and Accounting

In earlier Cisco IOS releases, only named authentication method lists were supported under Cisco's Authentication, Authorization, and Accounting (AAA) network security services. With Cisco IOS Release 11.3(3)T, AAA has been extended to support both authorization and accounting named method lists. Named Method Lists for AAA Authorization and Accounting function the same way as those for authentication: they allow you to define different methods for authorization and accounting and apply those methods on a per-interface or per-line basis.

Automated Double Authentication

The Automated Double Authentication feature enhances the previous double authentication feature. Previously with the double authentication feature, a second level of user authentication was achieved when you telnetted to the network access server or router and entered a username and password. Now, with automated double authentication, you do not have to telnet anywhere, but instead respond to a dialog box that requests a username and password or PIN.

Microsoft Point-to-Point Compression (MPPC)

Microsoft Point-to-Point Compression (MPPC) is a scheme used to compress Point-to-Point Protocol (PPP) packets between Cisco and Microsoft client devices. The MPPC algorithm is designed to optimize bandwidth utilization in order to support multiple simultaneous connections. The MPPC algorithm uses a Lempel-Ziv (LZ)-based algorithm with a continuous history buffer called a dictionary.

Multiple ISDN Switch Types

This feature allows you to configure more than one ISDN switch type per router. An ISDN switch type can be applied on a per-interface basis, thus extending the existing **global isdn switch-type** command to the interface level. This allows Basic Rate Interfaces (BRI) and Primary Rate Interfaces (PRI) to run simultaneously on platforms that support both interface types.

National ISDN Switch Types for BRI and PRI

National ISDN Switch Types for Basic Rate and Primary Rate Interfaces introduces changes to ISDN switch types for Primary Rate Interfaces (PRIs) and Basic Rate Interfaces (BRIs) as follows:

- Adds a new switch type for PRI interfaces (`isdn switch-type primary-ni`).
- Changes the BRI `basic-ni1` switch type to `basic-ni` (`isdn switch-type basic-ni`).
- Removes the ISDN `vn2` switch type (`isdn switch-type vn2`) used in France. The existing `vn3` switch type (`isdn switch-type vn3`) supports French `vn2` switches.
- Removes the ISDN `basic-nwnet3` switch type (`isdn switch-type basic-nwnet3`) used in Norway. The `basic-net3` switch type (`isdn switch-type basic-net3`) supports Norway NET3 switches.
- Removes the ISDN `basic-nznet3` switch type (`isdn switch-type basic-nznet3`) used by New Zealand NET3 switches. The ISDN `basic-net3` switch type (`isdn switch-type basic-net3`) supports New Zealand NET3 switches.
- Adds the ability to configure outgoing PRI B-channel selection for the T1 controller in ascending order (channel 1 to channel 23) or descending order (channel 23 to channel 1). Previously, the router selected a B-channel for outgoing calls from the highest free channel in descending order. The E1 controller channel selection for ascending order is channel 1 to 31, and 31 to 1 for descending order.

Note The command parser will still accept the following switch types: `basic-nwnet3`, `vn2`, and `basic-net3`; however, when viewing the NVRAM configuration using either the `show running configuration` or `write terminal` command, the `basic-net3` or `vn3` switch types are displayed respectively.

VPDN MIB and Syslog Facility

The Virtual Private Dialup Network (VPDN) Management Information Base (MIB) feature is intended to support all the tables and objects defined in the Cisco VPDN Management MIB for VPDN user sessions. VPDN system-wide information is available. This includes active VPDN tunnels, active user sessions in active VPDN tunnels, and failure history information, per username.

The VPDN Syslog facility provides generic logging output for VPDN information, such as Layer 2 Forwarding Protocol (L2F). The syslog messages are generated to inform authentication or authorization errors, resource issues, and time-out events.

Additional Vendor-Proprietary RADIUS Attributes

Remote Authentication Dial-In User Server (RADIUS) is an access server authentication, authorization, and accounting protocol originally developed by Livingston, Inc. Although an Internet Engineering Task Force (IETF) draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS, this Cisco IOS software release introduces support for the following additional RADIUS attributes:

- Multilink-ID
- Num-In-Multilink
- Pre-Input-Octets
- Pre-Output Octets
- Pre-Input Packets
- Pre-Output Packets
- Disconnect-Cause
- Date-Rate
- PreSession-Time

New Features in Cisco IOS Release 11.3(2)XA

The following hardware enhancements were introduced in Cisco IOS Release 11.3(2)XA and are available for the Cisco uBR7246.

MC11 Cable Modem Cards

The MC11 cable modem cards installed in the Cisco uBR7246 provide the connection to the HFC network. The MC11 modem cards offer one upstream port and one downstream port. The cable modem card slots are numbered from top to bottom: cable modem card slot3, slot4, slot5, and slot6.

Cisco uBR7246 Universal Broadband Router

Cisco uBR7246 universal broadband features enable the Cisco uBR7246 universal broadband router to communicate with a hybrid fiber coaxial cable (HFC) network via a Cisco MC11 cable modem card. Cisco MC11 cable modem cards allow you to connect cable modems on the HFC network to a Cisco uBR7246 in a Community Antenna Television (CATV) headend facility. The modem card provides the interface between the Cisco uBR7246 protocol control information (PCI) bus and the radio frequency (RF) signal on the HFC network.

No New Features in Cisco IOS Release 11.3(1)T

There were no new features introduced for the Cisco uBR7246 in Cisco IOS Release 11.3(1)T.

Important Notes

The following section contains important notes about Cisco IOS Release 11.3 that may apply to the Cisco uBR7246.

ATM Multipoint Signaling

Prior to Cisco IOS Release 11.1(13) and 11.2(8), the **atm multipoint-signaling** command was used on the main interface and affected all subinterfaces. For Release 11.1(13), 11.2(8), and later releases (including Release 11.3), explicit configuration on each subinterface is required to obtain the same functionality. Refer to caveat CSCdj20944, which is described as follows:

The **atm multipoint-signaling** interface command is currently only available on the main ATM interface. The effect is that signaling behavior (point-to-point or point-to-multipoint) for all clients on all subinterfaces is determined by the command on the main interface.

Clients on different subinterfaces can have different behavior. Specifically, RFC1577 requires point-to-point, and PIM allows point-to-multipoint. The command should be on a per-subinterface basis.

Enable the **atm multipoint-signaling** command on all subinterfaces that require it. Previously, you only needed to enable the command on the main interface.

Cisco IOS Release 11.3, 11.3 NA and 11.3 T End of Sales and End of Engineering

End of Engineering (EOE) means that there are no more regularly scheduled maintenance releases. The last maintenance release scheduled on the EOE date is only available through CCO and Field Service Operations—not through manufacturing.

Cisco IOS Releases 11.3, 11.3 NA, and 11.3 T reached End of Sales (EOS) status with maintenance Releases 11.3(10), 11.3(10)NA, 11.3(10)T. Releases 11.3, 11.3 NA, and 11.3 T will reach End of Engineering (EOE) with Releases 11.3(11), 11.3(11)NA, and 11.3(11)T.

Ongoing support for functionality in Releases 11.3, 11.3 NA, and 11.3 T is available in Cisco IOS Release 12.0(4)T and later maintenance releases of Cisco IOS Release 12.0.

For more information, see *End of Sales and End of Engineering for Cisco IOS Software Releases* product bulletins located on CCO and refer to the “Cisco Connection Online” section on page 27.

On CCO, click on this path:

Service & Support: Product Bulletins: Software

Under **Cisco IOS 11.3**, click on **End of Sales and End of Engineering for Cisco IOS Software Releases 11.3 and 11.3 T (#847: 12/98)** or **Cisco IOS Software 11.3 NA EoS and EoE (#849:12/98)**

Image Deferral, Cisco IOS Release 11.3(8)T

Cisco IOS Release 11.3(8)T was deferred to Release 11.3(8)T1 on all software images to incorporate corrections to the following caveats:

- CSCdk86294—The D channel is always in the shutdown state when non-facility associated signaling is configured.
- CSCdk80809—Enhanced Interior Gateway Routing Protocol (EIGRP) has difficulty converging on certain routes.

For more information on these caveats, refer to Bug Navigator II. Bug Navigator II is available at <http://www.cisco.com/support/bugtools>. On CCO, click this path:

Service & Support: Online Technical Support: Software Bug Toolkit: Bug Navigator II.

Enabling IPX Routing

Whenever IPX routing is enabled, the Token Ring interface resets.

Forwarding of Locally Sourced AppleTalk Packets

Cisco's implementation of AppleTalk does not forward packets with local-source and destination network addresses. This behavior does not conform to the definition of AppleTalk in Apple Computer's *Inside AppleTalk* publication. However, this behavior is designed to prevent any possible corruption of the AppleTalk Address Resolution Protocol (AARP) table in any AppleTalk node that collects MAC addresses.

Missing Source-Route Bridging Commands

Due to a production problem, many source-route bridging commands were omitted from the printed version of the *Cisco IOS Software Command Summary (78-4746-XX)*. For documentation of all source-route bridging commands, refer to the *Bridging and IBM Networking Command Reference (78-4743-XX)*. You can also obtain the most current documentation on CCO or on the Documentation CD-ROM.

New TACACS+ Attribute-Value Pair

A new authorization feature that allows you to separately configure and authorize Multilink PPP was added in Cisco IOS Release 11.3(1). This feature can cause MLP authorization to fail in TACACS+ servers that do not include the relevant authorization permissions in the configuration.

For TACACS+, add the following attribute-value (AV) pair for all users who are allowed to negotiate Multilink PPP:

```
service = ppp protocol = multilink {
```

Using LAN Emulation

Note the following information regarding the LAN Emulation (LANE) feature in Cisco IOS Release 11.3:

- LANE is available for use with Cisco 4500 and Cisco 4700 series routers, and Cisco 7000 and Cisco 7500 series routers connected to either an LS100 or LS1010 switch. LANE requires at least Version 3.1(2) of the LS100 software, which requires a CPU upgrade if you are currently running software earlier than Version 2.5.
- Do not use the LS2020 for LANE because it does not support UNI 3.0 and point-to-multipoint SVCs.
- Routing of IP, IPX, AppleTalk, DECnet, VINES, and XNS is supported.
- Hot Standby Router Protocol (HSRP) is supported.
- LANE does not support Connectionless Network Service (CLNS) or LANE over Permanent Virtual Circuits (PVCs).
- Do not route AppleTalk Phase 1 to AppleTalk Phase 2 using LANE.

40-bit Encryption Images are Unavailable in Release 11.3(1)

Cisco is conducting an internal review of the build and distribution processes associated with its 40-bit Cisco IOS cryptographic products. To provide seamless access to Cisco IOS 40-bit encryption capability, Cisco will provide access to the most current 40-bit encryption images, beginning with Cisco IOS Release 11.2 (12), 11.2(12)P, and 11.3(2).

The following 40-bit encryption images are unavailable indefinitely:

- 11.2(1)–11.2(11.2)
- 11.2(2)P–11.2(11.1)P
- 11.2(1)F–11.2(4)F
- 11.3(1)

This review is not related to any new or previously unreported caveats. The information gathered in the review will be used to implement new automated development and order-processing applications.

Cisco IOS Syslog Failure

Certain releases of Cisco IOS software may fail or hang when they receive invalid User Datagram Protocol (UDP) packets sent to their syslog ports (port 514). At least one commonly-used Internet scanning tool generates packets that can cause such problems. This fact has been published on public Internet mailing lists, which are widely read both by security professionals and by security attackers. This information should be considered in the public domain.

Attackers can cause Cisco IOS devices to repeatedly fail and reload, resulting in a completely disabled Cisco IOS device that will need to be reconfigured by its administrator. Some Cisco IOS devices have been observed to hang instead of failing when attacked. These devices do not recover until they are manually restarted by reset or power cycling. An administrator must personally visit an attacked, hung device to restart it, even if the attacker is no longer actively sending any traffic. Some devices have failed without providing stack traces; some devices may indicate that they were “restarted by power-on,” even when that is not the case.

Assume that any potential attacker is likely to know that existence of this vulnerability and the ways to exploit it. An attacker can use tools available to the public on the Internet and does not need to write any software to exploit the vulnerability. Minimal skill is required and no special equipment is required.

Despite Cisco specifically inviting such reports, Cisco has received no actual reports of malicious exploitation of this vulnerability.

This vulnerability notice was posted on Cisco's World Wide Web site:

<http://www.cisco.com/warp/public/770/iossyslog-pub.shtml>

This information was also sent to the following e-mail and Usenet news recipients:

- cust-security-announce@cisco.com
- bugtraq@netspace.org
- first-teams@first.org (includes CERT/CC)
- first-info@first.org
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- nanog@merit.edu

Affected Devices and Software Releases

Vulnerable devices and software releases are specified in Table 6, *Affected and Repaired Software Releases*. Affected releases include Releases 11.3 AA, 11.3 DB, and all 12.0 releases (including 12.0 mainline, 12.0 S, 12.0 T, and any other regular released version whose number starts with 12.0), up to the repaired releases listed in Table 6. Cisco is correcting the vulnerability in certain special releases, will correct it in future maintenance and interim releases, and intends to provide fixes for all affected IOS variants. See Table 6, *Affected and Repaired Software Releases* for details.

No particular configuration is needed to make a Cisco IOS device vulnerable. It is possible to filter out attack traffic by using access lists. See the "Workarounds" section on page 17 for techniques. However, except at Internet firewalls, the appropriate filters are not common in customer configurations. Carefully evaluate your configuration before assuming that any filtering you have protects you against this attack.

The most commonly used or asked-about products are listed below. If you are unsure whether your device is running Cisco IOS software, log in to the device and issue the **show version** command. Cisco IOS software will identify itself simply as "IOS" or "Internetwork Operating System Software". Other Cisco devices will not have the **show version** command, or they will identify themselves differently in their output. The most common Cisco devices that run Cisco IOS software include the following:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800,ubr900, 1000, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200 (including the ubr7200), 7500, and 12000 series
- Most recent versions of the LS1010 ATM switch
- Some versions of the Catalyst 2900XL LAN switch
- Cisco DistributedDirector

Affected software releases, which are relatively new, are not necessarily available on every device listed above. If you are not running Cisco IOS software, you are not affected by this vulnerability.

The following Cisco devices are *not* affected:

- 700 dialup routers (750, 760, and 770 series)
- Catalyst 1900, 2800, 2900, 3000, and 5000 LAN switches, except for some versions of the Catalyst 2900XL. However, optional router modules running Cisco IOS software in switch backplanes, such as the RSM module for the Catalyst 5000 and 5500, are affected.
- WAN switching products in the IGX and BPX lines
- MGX (formerly known as the AXIS shelf)
- Host-based software
- Cisco PIX Firewall
- Cisco LocalDirector
- Cisco Cache Engine

This vulnerability has been assigned Cisco bug ID CSCdk77426.

Solution

Cisco offers free software updates to correct this vulnerability for all affected customers—regardless of their contract status. However, because this vulnerability information has been disseminated by third parties, Cisco has released this notice before updates are available for all software releases. Table 6 gives Cisco’s projected fix dates.

Make sure your hardware had adequate RAM to support the new software before installing it. The amount of RAM is seldom a problem when you upgrade within a major release (say, from 11.2(11)P to 11.2(17)P), but it is often a factor when you upgrade between major releases (say, from 11.2 P to 11.3 T).

Because fixes will be available for all affected releases, this vulnerability will rarely, if ever, require an upgrade to a new major release. Cisco recommends very careful planning for any upgrade between major releases. Make certain no known bugs will prevent the new software from working properly in your environment.

Further upgrade planning assistance is available on Cisco’s World Wide Web site at:

<http://www.cisco.com>

If you have service contracts you can obtain new software through your regular update channels (generally via Cisco’s World Wide Web site). You can upgrade to any software release, but you must remain within the boundaries of the feature sets you have purchased.

If you don’t have service contracts, you can upgrade to obtain only the bug fixes; free upgrades are restricted to the minimum upgrade required to resolve the defects. In general, you will be restricted to upgrading within a single row of Table 6, except when no upgrade within the same row is available in a timely manner. Obtain updates by contacting one of the following Cisco Technical Assistance Centers (TACs):

- +1 800 553 2447 (toll-free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- tac@cisco.com

Give the URL of this notice (<http://www.cisco.com/warp/public/770/iossyslog-pub.shtml>) as evidence for a free update. Non-contract customers must request free updates through the TAC. Please do not contact either “psirt@cisco.com” or “security-alert@cisco.com” for software updates.

Workarounds

You can work around this vulnerability by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to its port 514. This can be done either using packet filtering on surrounding devices, or by using input access list filtering on the affected IOS device itself.

If you use an input access list, apply that list to all interfaces to which attackers may be able to send datagrams. Interfaces include—not only physical LAN and WAN interfaces—but virtual subinterfaces of those physical interfaces, as well as virtual interfaces and interface templates corresponding to GRE, L2TP, L2F, and other tunneling protocols.

The input access list must block traffic destined for UDP port 514 at any of the Cisco IOS device's own IP addresses, as well as at any broadcast or multicast addresses on which the Cisco IOS device may be listening. Be sure to block both old-style “all-zeros” broadcasts and new-style “all-ones” broadcasts. It is not necessary to block traffic being forwarded to other hosts—only traffic actually addressed to the Cisco IOS device is of interest. No single input access list works in all configurations. Know the effect of your access list in your specific configuration before activating it.

The following example shows a possible access list for a three-interface router, along with the configuration commands needed to apply the list. The example assumes input filtering is not needed, other than as a workaround for this vulnerability:

```

! Deny all multicasts, and all unspecified-net broadcasts, to port 514
access-list 101 deny udp any 224.0.0.0 31.255.255.255 eq 514
! Deny old-style unspecified-net broadcasts
access-list 101 deny udp any host 0.0.0.0 eq 514
! Deny network-specific broadcasts. This example assumes that all of
! the local interfaces are on the class B network 172.16.0.0, subnetted
! everywhere with mask 255.255.255.0. This will differ from network
! to network. Note that we block both new-style and old-style broadcasts.
access-list 101 deny udp any 172.16.0.255 0.0.255.0 eq 514
access-list 101 deny udp any 172.16.0.0 0.0.255.0 eq 514
! Deny packets sent to the addresses of our own network interfaces.
access-list 101 deny udp any host 172.16.1.1 eq 514
access-list 101 deny udp any host 172.16.2.1 eq 514
access-list 101 deny udp any host 172.16.3.3 eq 514
! Permit all other traffic (default would be to deny)
access-list 101 permit ip any any

! Apply the access list to the input side of each interface
interface ethernet 0
ip address 172.16.1.1 255.255.255.0
ip access-group 101 in

interface ethernet 2
ip address 172.16.2.1 255.255.255.0
ip access-group 101 in

interface ethernet 3
ip address 172.16.3.3 255.255.255.0
ip access-group 101 in

```

Listing all possible addresses—especially all possible broadcast addresses—to which attack packets may be sent is complicated. If you do not need to forward any legitimate syslog traffic received on an interface, you can block all syslog traffic arriving on that interface. Remember that blocking will affect traffic routed through the Cisco IOS device as well as traffic destined to the device; if the IOS device is expected to forward syslog packets, you will have to do the detailed filtering. Because input access lists impact system performance, install them with caution—especially on systems running very near their capacity.

Software Versions and Fixes

Many Cisco software images have been or will be specially reissued to correct this vulnerability. For example, regular released version 12.0(2) is vulnerable, as are interim releases 12.0(2.1) through 12.0(2.3). The first fixed interim version of 12.0 mainline software is 12.0(2.4). However, a special release, 12.0(2a), contains only the fix for this vulnerability and does not include any other bug fixes from later 12.0 interim releases.

If you are running 12.0(2) and want to fix this problem without risking possible instability presented by installing the 12.0(2.4) interim release, you can upgrade to 12.0(2a). Release 12.0(2a) is a “code branch” from the 12.0(2) base, which will merge back into the 12.0 mainline at 12.0(2.4).

Special releases, like 12.0(2a), are one-time, spot fixes, and they will not be maintained. Thus, the upgrade path from 12.0(2a) is to 12.0(3).

Table 6 specifies information about affected and repaired software releases.

Note All dates within this table are subject to change.

Table 6 Affected and Repaired Software Releases

Cisco IOS Major Release	Description	Special Fix¹	First Fixed Interim Release²	Fixed Maintenance Release³
Unaffected Releases				
11.2 and earlier releases—all variants	Unaffected early releases (no syslog server)	Unaffected	Unaffected	Unaffected
11.3, 11.3 T, 11.3 DA, 11.3 MA, 11.3 NA, 11.3 WA, 11.3(2)XA	11.3 releases without syslog servers	Unaffected	Unaffected	Unaffected
Releases based on 11.3				
11.3 AA	11.3 early deployment for AS58xx	11.3(7)AA2, 8-JAN-1999 ⁴	11.3(7.2)AA	11.3(8)AA, 15-FEB-1999
11.3 DB	11.3 for Cisco NRP routing blade in Cisco 6400 xDSL DSLAM			11.3(7)DB2, 18-JAN-1999
Releases based on 12.0				
12.0	12.0 Mainline	12.0(2a), 8-JAN-1999	12.0(2.4)	12.0(4), 12-APR-1999
12.0 T	12.0 new technology early deployment	12.0(2a)T1, 11-JAN-1999	12.0(2.4)T	12.0(3)T, 15-FEB-1999
12.0 S	ISP support; 7200, RSP, GSR		12.0(2.3)S, 27-DEC-1998	12.0(2)S ⁵ , 18-JAN-1999
12.0 DB	12.0 for Cisco 6400 universal access concentrator node switch processor (lab use)			12.0(2)DB, 18-JAN-1999
12.0(1)W	12.0 for Catalyst 8500 and LS1010	12.0(1)W5(5a) and 12.0(1a)W5(5b) (LS1010 platform only)	12.0(1)W5(5.15)	12.0(1)W5(6) (platform support for Catalyst 8540M will be in 12.0(1)W5(7))

Table 6 Affected and Repaired Software Releases (continued)

Cisco IOS Major Release	Description	Special Fix ¹	First Fixed Interim Release ²	Fixed Maintenance Release ³
12.0(0.6)W5	One-time early deployment for CH-OC12 module in Catalyst 8500 series switches	Unaffected; one-time release	Unaffected	Unaffected; To upgrade use 12.0(1)W5 releases.
12.0(1)XA3	Short-life release; merged to 12/0T at 12.0(2)T	Obsolete	Merged	Upgrade to 12.0(2a)T1 or to 12.0(3)T.
12.0(1)XB	Short-life release for Cisco 800 series; merged to 12.0 T and 12.0 (3)T	12.0(1)XB1	Merged	Upgrade to 12.0(3)T.
12.0(2)XC	Short-life release for new features in Cisco 2600, Cisco 3600, ubr7200, ubr900 series; merged to 12.0 T at 12.0(3)T	12.0(2)XC1, 7-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(2)XD	Short-life release for ISDN voice features; merged to 12.0 T at 12.0(3)T	12.0(2)XD1, 18-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(1)XE	Short-life release	12.0(2)XE, 18-JAN-1999	Merged	Upgrade to 12.0(3)T

1 A special fix is a one-time release that provides the most stable immediate upgrade path.

2 Interim releases are tested less rigorously than regular maintenance releases; interim releases can contain serious bugs.

3 Fixed maintenance releases are on a long-term upgrade path. Other long-term upgrade paths also exist.

4 All dates in this table are estimates and are subject to change.

5 This entry is not a misprint. The 12.0(2.3)S interim release is available before the 12.0(2)S regular release.

Deprecated MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. OLD-CISCO-* MIBs are currently being migrated into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in the following table.

Table 7 **Deprecated and Replacement MIBs**

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	In Development
OLD-CISCO-DECNET-MIB	
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBS)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

For information on caveats in Cisco IOS Release 11.3 T, refer to the *Caveats for Cisco IOS Release 11.3 T* document. This document lists severity 1 and 2 caveats for all releases of Cisco IOS Release 11.3 T. The caveats document is located on CCO and the Documentation CD-ROM.

Because Cisco IOS Release 11.3 T is based on Cisco IOS Release 11.3, all caveats in Release 11.3 are also in Release 11.3 T. For information on caveats in Cisco IOS Release 11.3, refer to the “Important Notes and Caveats for Release 11.3” section in the cross-platform *Release Notes for Cisco IOS Release 11.3* document which is located on CCO and the Documentation CD-ROM. These release notes list severity 1 and 2 caveats affecting all maintenance releases.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. From CCO, log in, and click on this path: **Service & Support: Online Technical Support: Software Bug Toolkit**. You can also find Bug Navigator II at <http://www.cisco.com/support/bugtools>.

Related Documentation

This section describes the documentation available for the Cisco uBR7246. These documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are only available online on CCO and on the Documentation CD-ROM.

Use these release notes with the documents listed in the following sections:

- Release-Specific Documents, page 21
- Platform-Specific Documents, page 22
- Feature Modules, page 22
- Cisco IOS Software Documentation Set, page 23

Release-Specific Documents

The following documents are specific to Release 11.3. They are located on CCO and the Documentation CD-ROM:

- *Release Notes for Cisco IOS Release 11.3*

To reach the cross-platform *Release Notes for Cisco IOS Release 11.3* from the CCO home page, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Product-Specific Release Notes for Cisco IOS Release 11.3

To reach the cross-platform *Release Notes for Cisco IOS Release 11.3* on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Product Specific Release Notes for Cisco IOS Release 11.3: Cross-Platform Release Notes for Cisco IOS Release 11.3

- Product bulletins, field notices, and other release-specific documents

To reach these documents from the CCO home page, click on this path:

Service & Support: Technical Documents

- Caveats document

As a supplement to the caveats listed in the “Caveats” section on page 20 of these release notes, refer to the *Caveats for Cisco IOS Release 11.3 T* document, which contains caveats applicable to all platforms for all maintenance releases of Release 11.3 T.

To reach the Caveats document from CCO, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T

To reach the Caveats document on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. From CCO, log in, and click on this path: **Service & Support: Online Technical Support: Software Bug Toolkit**. You can also find Bug Navigator II at <http://www.cisco.com/support/bugtools>.

Platform-Specific Documents

The documents listed in this section are available for the Cisco uBR7246 and Cisco uBR904.

- Cisco uBR7246 Platform Documentation
 - *Cisco uBR7246 Installation and Configuration Guide*
 - *Cisco uBR7200 Series Configuration Notes*
 - *Cisco Network Registrar for the uBR7200 Series*
 - *Regulatory and Safety Compliance for the Cisco uBR7246*
 - *Cisco uBR7200 Series Features*
 - *Cisco uBR7200 Series Feature Enhancements*
- Cisco uBR904 Platform Documentation
 - *Cisco uBR904 Installation and Configuration Guide*
 - *Update to the uBR904 Cable Modem Installation and Configuration Guide*
 - *Bridging and Routing Features for the Cisco uBR904 Cable Modem*
 - *Regulatory Compliance and Safety Information for the Cisco uBR904*
 - *Troubleshooting Tips for the Cisco uBR904 Cable Modem*
 - *Cisco uBR904 Cable Modem Subscriber Setup Quick Reference Card*

To reach Cisco uBR7200 and Cisco uBR900 series documentation on CCO, follow this path:

Service and Support: Documentation Home Page: Broadband/Cable Solutions: Cisco uBR7200 Series Universal Broadband Routers or Cisco uBR900 Series Cable Modems

To reach Cisco uBR7200 and Cisco uBR900 series documentation on the Documentation CD-ROM, follow this path:

Cisco Product Documentation: Broadband/Cable Solutions: Cisco uBR7200 Series Universal Broadband Routers or Cisco uBR900 Series Cable Modem

Feature Modules

Feature modules describe new features supported by Release 11.3 and are updates to the Cisco IOS documentation set. Feature modules consist of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the features modules are available online only. The feature module information is included in the next printing of the Cisco IOS documentation set.

To reach the feature modules on the CCO home page, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3: New Features in Release 11.3

To reach the feature modules on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3: New Features in Release 11.3

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. These documents are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use the configuration guide with its corresponding command reference.

On CCO and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set: configuration guides and command references.

To reach these documents on the CCO home page, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3 Configuration Guides, Command References: Configuration Guide Master Index or Command Reference Master Index

To reach these documents on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3 Configuration Guides, Command References: Configuration Guide Master Index or Command Reference Master Index

Release 11.3 Documentation Set

Table 8 describes the contents of the Cisco IOS Release 11.3 software documentation set. The document set is available in electronic form, and also in printed form upon request.

Note You can find the most current Cisco IOS documentation on the latest Documentation CD-ROM and on the Web. These electronic documents may contain updates and modifications made after the paper documents were printed.

To reach software documents from the CCO home page, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3

To reach software documentation on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3

Related Documentation

Table 8 Cisco IOS Software Release 11.3 Documentation Set

Books	Chapter Topics
<ul style="list-style-type: none">• Configuration Fundamentals Configuration Guide• Configuration Fundamentals Command Reference	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none">• Network Protocols Configuration Guide, Part 1• Network Protocols Command Reference, Part 1	IP Addressing IP Services IP Routing Protocols
<ul style="list-style-type: none">• Network Protocols Configuration Guide, Part 2• Network Protocols Command Reference, Part 2	AppleTalk Novell IPX
<ul style="list-style-type: none">• Network Protocols Configuration Guide, Part 3• Network Protocols Command Reference, Part 3	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none">• Wide-Area Networking Configuration Guide• Wide-Area Networking Command Reference	ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none">• Security Configuration Guide• Security Command Reference	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options
<ul style="list-style-type: none">• Cisco IOS Interface Configuration Guide• Cisco IOS Interface Configuration Guide	Interface Configurations
<ul style="list-style-type: none">• Dial Solutions Configuration Guide• Dial Solutions Command Reference	Dial-In Port Setup Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions ISDN X.25 over ISDN VPDN Dial Business Solutions and Examples
<ul style="list-style-type: none">• Cisco IOS Switching Services Configuration Guide• Cisco IOS Switching Services Command Reference	Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing

Table 8 Cisco IOS Software Release 11.3 Documentation Set (continued)

Books	Chapter Topics
<ul style="list-style-type: none"> • Bridging and IBM Networking Configuration Guide • Bridging and IBM Networking Command Reference 	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set
<ul style="list-style-type: none"> • Voice, Video, and Home Applications Configuration Guide • Voice, Video, and Home Applications Command Reference 	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Video Support Universal Broadband Features
<ul style="list-style-type: none"> • Quality of Service Solutions Configuration Guide • Quality of Service Solutions Command Reference 	Classification Scheduling Packet Drop Traffic Shaping ATM QoS SNA QoS Line Protocols
<ul style="list-style-type: none"> • Configuration Guide Master Index • Command Reference Master Index 	
<ul style="list-style-type: none"> • Cisco IOS Software Command Summary • Cisco IOS System Error Messages • Debug Command Reference • Dial Solutions Quick Configuration Guide 	

Note The *Cisco Management Information Base (MIB) User Quick Reference* publication is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco Connection Online. From CCO, click on the following path: **Software & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB.**

Service and Support

For service and support for a product purchased from a reseller, contact the reseller. Resellers offer a wide variety of Cisco service and support programs, which are described in the section “Service and Support” in the information packet that shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems’ primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a CCO login account, you can access the following URL, which contains links and helpful tips on configuring Cisco products:

http://www.cisco.com/kobayashi/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path: **Products & Technologies: Products: Technical Tips**

The following sections are provided from the Technical Tips page:

- Access Dial Cookbook—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Designed to notify you of any critical issues regarding Cisco products. These notices include problem descriptions, safety or security issues, and hardware defects.
- Hardware—Technical Tips related to specific hardware platforms.
- Hot Tips—Popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.
- Internetworking Features—Tips on using and deploying Cisco IOS software features and services.
- Sample Configurations—Actual configuration examples—examples complete with topology and annotations.
- Software Products—MultiNet & Cisco Suite 100, Network Management, Cisco IOS Software Bulletins, and CiscoPro Configurations.
- Special Collections—Other Helpful Documents, including Case Studies, References & RFCs, and Security Advisories.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

This document is to be used with the documents in the "Related Documentation," page 21.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, CiscoLink, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Technologies logo, ConnectWay, ControlStream, Fast Step, FireRunner, GigaStack, IGX, JumpStart, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, Packet, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, ServiceWay, SlideCast, SMARTnet, StreamView, The Cell, TrafficDirector, TransPath, ViewRunner, VirtualStream, VisionWay, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9907R)

Copyright © 1999, Cisco Systems, Inc.